



A minha informação está segura?
Dicas para proteção da informação.

#ProtegeOTeuCampus

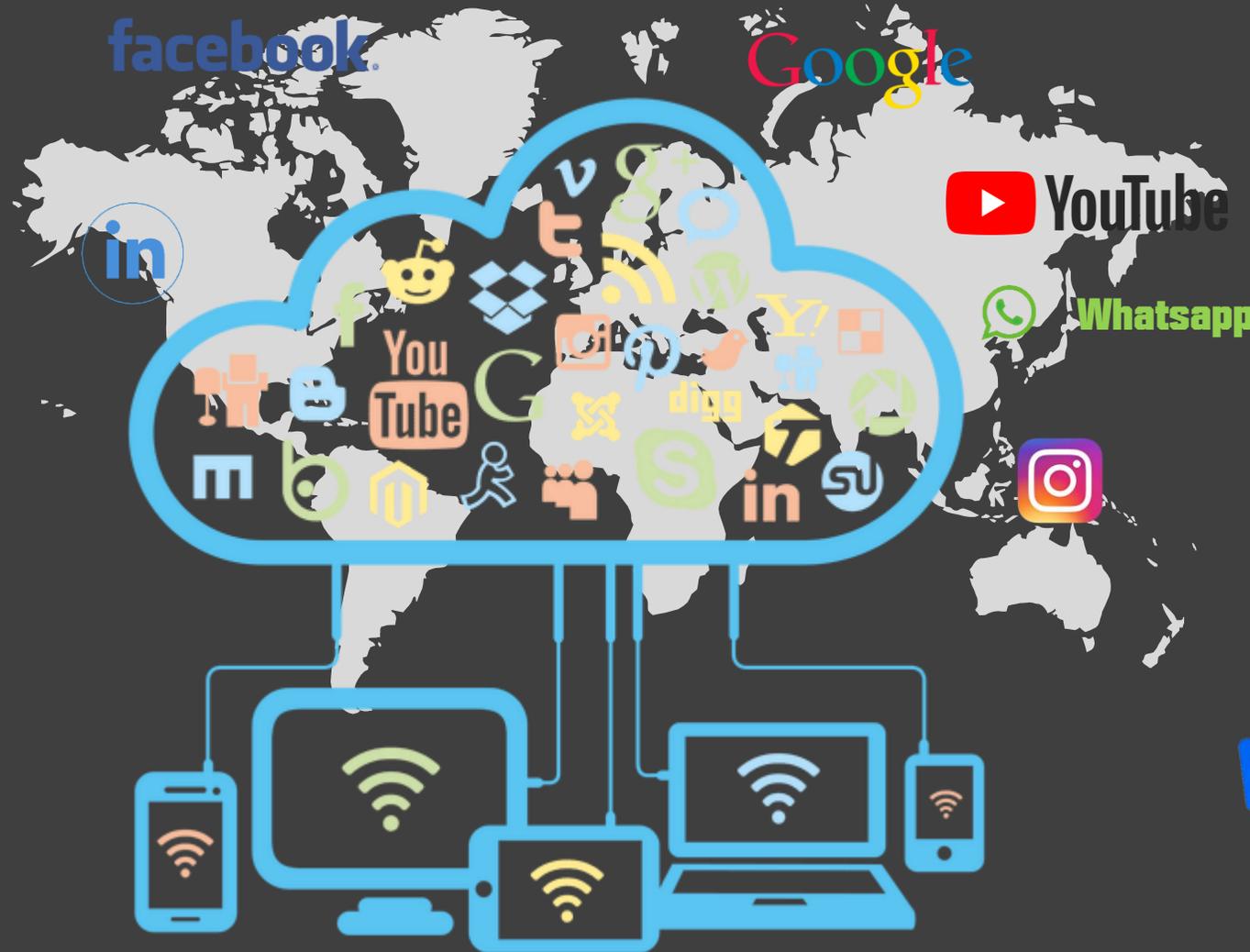
Internet

- Em janeiro de 2022, havia mais de 5 mil milhões de utilizadores da Internet.

- O utilizador médio global passa 6 horas e 43 minutos *online* todos os dias.

- Em dezembro de 2021, já existiam cerca de 2 mil milhões de *sites*.

- Prevê-se que as vendas globais de comércio eletrónico *online* atinjam os 5 biliões de dólares até ao final do ano.



Trajetos de informação



Metadados



- São dados alargados que nos permitem obter informações específicas do utilizador;
- Permitem identificar uma pessoa ou entidade;
- Podem ser utilizados para:
 - exposição geográfica;
 - obter informação sobre um site e/ou versões de software;
 - obter mensagens e documentos;

ATAQUE INFORMÁTICO

Hospital Garcia de Orta assegura que foi mantida "praticamente toda a atividade clínica"

“Já houve oito grandes ataques informáticos” este ano em Portugal. Em dois, “foi tudo destruído”

Ordem dos Engenheiros sofreu ataque informático que não...

Segurança Social atacada: dados de cidadãos e empresas podem estar em risco

Ciberataques: Laboratórios Germano de Sousa mantêm-se encerrados

Dados médicos privados expostos após ataque informático na Austrália

EUA propõem colaboração com Portugal após ciberataque na Defesa

Revolut sofre ciberataque e dados de 50 mil clientes ficam...

Hackers que atacaram SIC e Expresso dizem ter pirateado site do Parlamento

Portugal é o 31.º país mais afetado por ataques de ransomware

2022 foi um “ano terrível” para a cibersegurança em Portugal e especialistas avisam que 2023 pode ser pior



Fátima Caçador

casa.bits

28 out 2022 13:45

Computadores

ataque informático · cibersegurança · cncs · hacker · vulnerabilidade



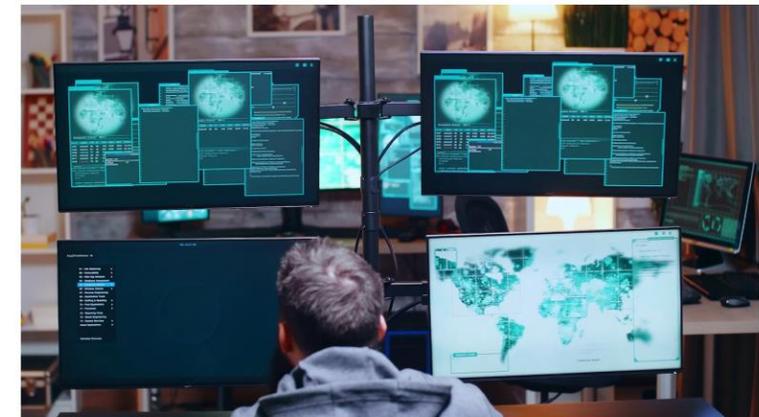
Computadores · 28 out 2022 16:24
Anatomia de um ataque: a dia em que a Vodafone Portugal recuou ao passado e teve de usar o 2G



Internet · 26 out 2022 07:17
Ataques para destruir ou paralisar infraestruturas elétricas estão a aumentar na Europa

Impresa, Vodafone, Hospital Garcia da Horta, Sonae, BCP, EMGFA, TAP. Estas são algumas das organizações que este ano sofreram ataques de grandes dimensões e foram alvo de roubo de informação, em alguns sem recuperação, uma situação que é vista como um alerta para a necessidade de investir em cibersegurança defensiva mas também ofensiva.

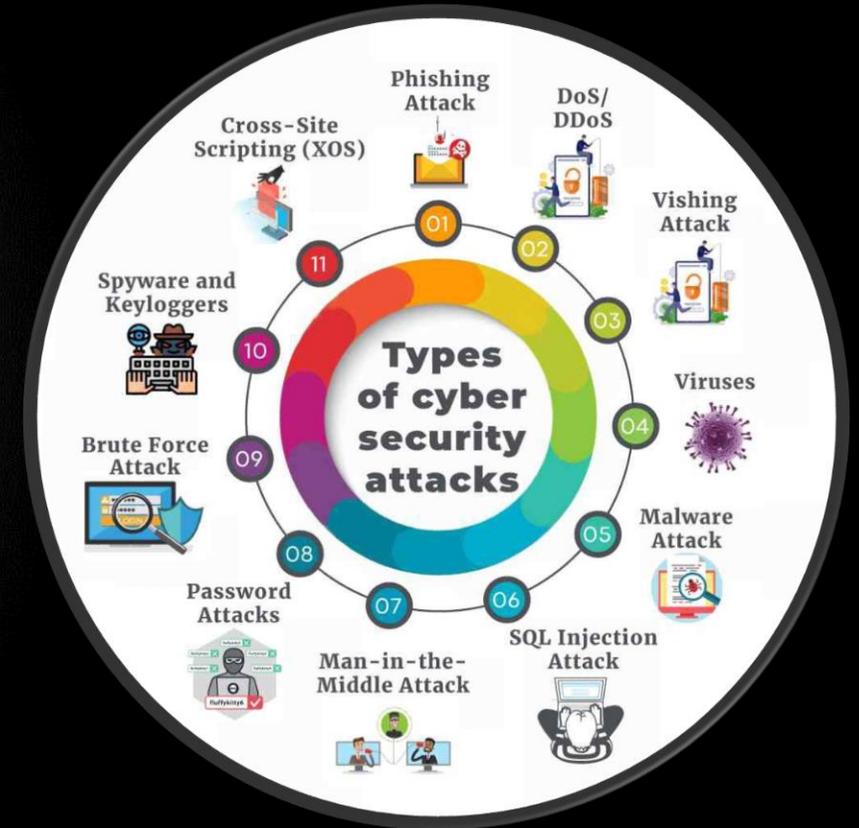
PUB
PUB
PUB



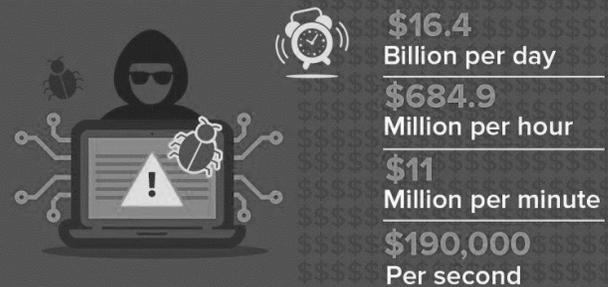
O ano começou com um sobressalto. Logo no dia 2 de janeiro a Impresa, dona da SIC e do Expresso, dá conta de um ataque informático que impedia o acesso aos sites da TV e do jornal e à plataforma OPTO, mas que afetou também os sistemas internos e o arquivo de informação. A gravidade do ataque do Lapsus\$ group foi sendo percebida ao longo dos dias seguintes, com a

Vodafone Portugal foi alvo de ataque informático

Tipos de ataque



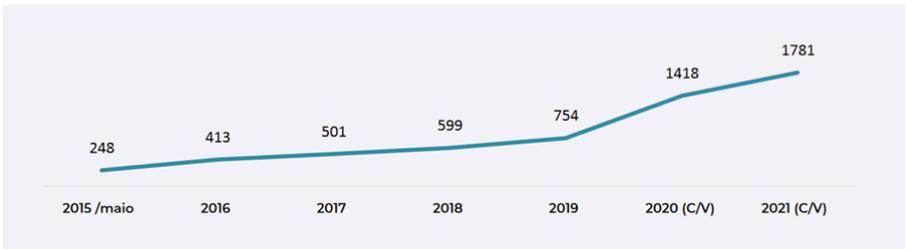
Global Cybercrime Damage by 2021



Source: Cybersecurity Ventures, 2020

Evolução de ataques em Portugal

Número de incidentes registados pelo CERT.PT, entre 2015 e 2021*



O *phishing/smishing* (40% dos incidentes), a engenharia social (14%) e a distribuição de *malware* (13%) foram os tipos de incidentes mais registado pelo CERT.PT em 2021 (CERT.PT – Equipa de Resposta a Incidentes de Segurança Informática Nacional).

* C/V: contabilizando as vulnerabilidades como incidentes (a partir de 2020).

Figura 2 | CERT.PT

+ 26% em 2021 relativamente a 2020.

Consultar *Relatório Cibersegurança em Portugal, Riscos e Conflitos 2022* (CNCS, 2022) para esclarecimento de conceitos:
<https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cnccs.pdf>



RK	Origem dos incidentes	Nº	%
1º	Falha humana	77	24
2º	Ransomware	70	22
3º	Ações fraudulentas (utilização indevida de recursos, usurpação de identidade)	42	13
4º	Phishing/Engenharia Social	38	12
5º	Falhas aplicacionais (desenho, implementação e/ou configuração)	32	10
6º	Exploração de outras vulnerabilidades	30	9
7º	Outras	12	4
8º	Perda ou furto de equipamento	9	3
9º	Malware	8	3

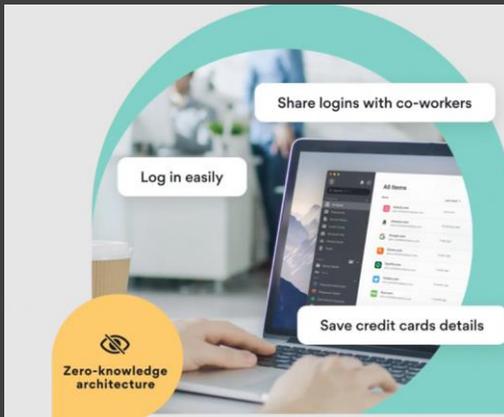
2020		2021		2020		2021		Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Tendência absoluta %	Lugar RK
1º	Phishing/smishing	613	43	1º	Phishing/smishing	715	40	+ 17	=
2º	Sistema infetado (malware)	169	12	2º	Engenharia social	246	14	+ 2136	+
3º	Distribuição de malware	119	8	3º	Distribuição de malware	226	13	+ 90	=
4º	Comprometimento de conta não privilegiada	111	8	4º	Comprometimento de conta não privilegiada	114	6	+ 2,7	=
5º	Acesso não autorizado	58	4	5º	Utilização ilegítima de nome de terceiros	80	4	+ 150	+
6º	Comprometimento de aplicação	55	4	6º	Indeterminado (outro)	50	3	+ 79	+
7º	Sistema vulnerável (vulnerabilidade)	41	3	7º	Sistema infetado (malware)	46	3	- 73	-
8º	Utilização ilegítima de nome de terceiros	32	2	8º	Sistema vulnerável (vulnerabilidade)	44	2	+ 7	-
9º	Indeterminado (outro)	28	2	9º	Modificação não autorizada (35 ransomware) *	38	2	+ 111	+
10º	Tentativa de login	26	2	10º	Exploração de Vulnerabilidade (tent. Intrusão)	37	2	+ 61	+

Informação e Alertas: <https://dyn.cnccs.gov.pt/pt/alertas>

Utilização de *passwords*

As palavras-passe mais usadas em Portugal podem ser desvendadas por um hacker em menos de um segundo.

1. Verifique todas as contas que possui, apagando as que não utiliza;
2. Utilize *passwords* longas e únicas - combinações de números, letras maiúsculas, minúsculas e símbolos;
3. Utilize senhas diferentes para cada conta;
4. Utilize um gestor de *passwords*.



Muitos dos incidentes de segurança cibernética acontecem por causa de simples erros humanos: deixar as suas senhas acessíveis a outras pessoas e/ou guardar em ficheiros de Excel ou outras aplicações não encriptadas.

[Lista das 200 passwords mais comuns](#)

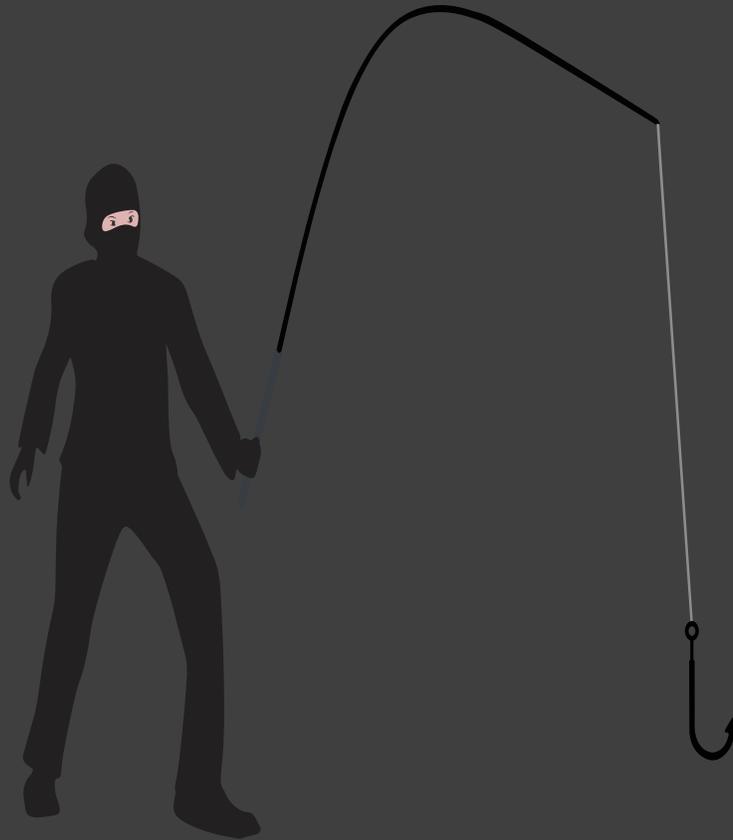
"Tal como todos que utilizam email, recebo toneladas de spam todos os dias. Muitos deles oferecem ajuda para sair das dívidas rapidamente. Seria engraçado se não fosse tão instigante." - Bill Gates

Regras básicas de Proteção

-  Use sempre sistemas atualizados e protegidos
-  Cumpra as regras definidas pela equipa de TI
-  Proteja a sua informação e identidade
-  Utilize senhas longas e complexas
-  Verifique as fontes para *download* de programas
-  Valide remetentes de *emails* e anexos
-  Confirme e utilize *sites* seguros para pagamentos



Exemplo de ataque de *phishing*



<https://youtu.be/7BY8Mae-3pg>

Gestores de passwords:

- KeePass
- Enpass Password Manager
- Avira Password Manager
- Norton Password Manager
- NordPass
- PassHub
- Bitwarden
- LogMeOnce Password Management Suite

Software de encriptação:

- Windows Bitlocker
- Folder Lock
- AxCrypt
- VeraCrypt
- SecureIT
- PixelCryptor

Informação e avaliações

<https://www.pcmag.com/picks/the-best-encryption-software>

<https://www.techradar.com/best/best-encryption-software>

<https://privacysavvy.com/security/safe-browsing/free-encryption-software>

<https://www.pcmag.com/picks/the-best-free-password-managers>

<https://www.pcmag.com/picks/the-best-password-managers>

Obrigado

sergio.peres@sapo.pt